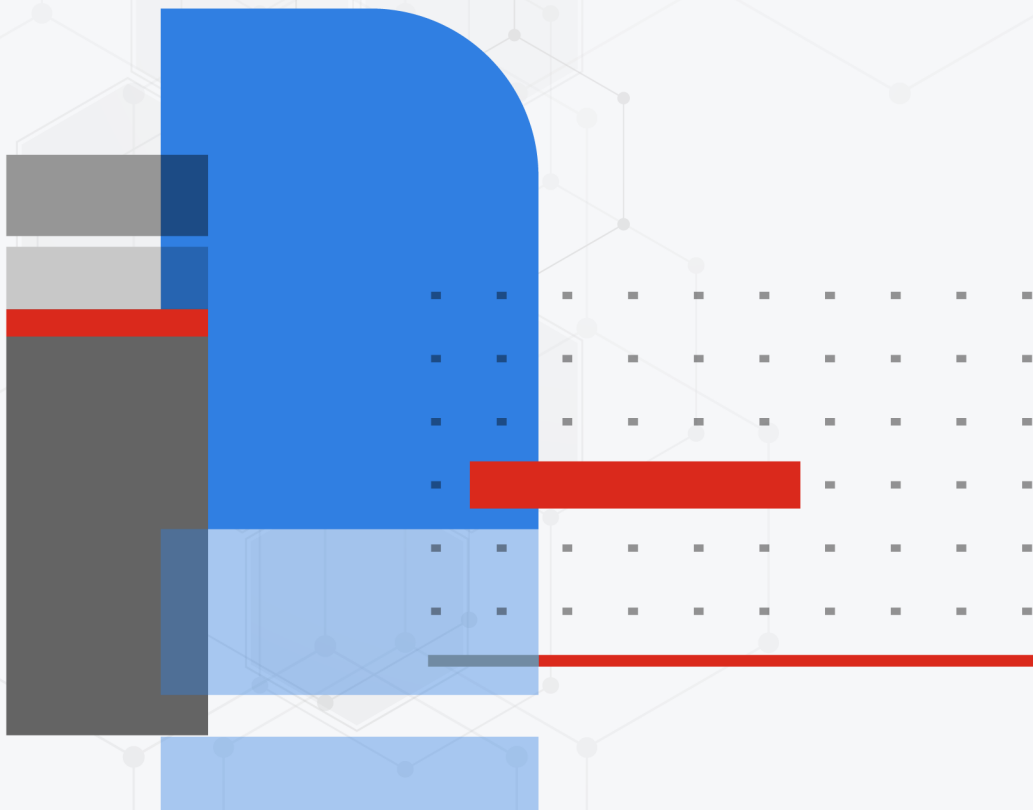




FortiLink Release Notes

FortiSwitchOS 7.4.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



October 4, 2023

FortiSwitchOS 7.4.1 FortiLink Release Notes

11-741-923190-20231004

TABLE OF CONTENTS

Change log	4
Introduction	5
What's new in FortiOS 7.4.1	6
Special notices	7
Support of FortiLink features	7
Upgrade information	8
Product integration and support	9
FortiSwitchOS 7.4.1 support	9
Resolved issues	10
Known issues	11

Change log

Date	Change Description
August 31, 2023	Initial document release for FortiOS 7.4.1
September 4, 2023	Corrected the release build number.
September 7, 2023	Updated the “What’s new in FortiOS 7.4.1” section.
October 2, 2023	Removed bug 907536.
October 4, 2023	Updated the “What’s new in FortiOS 7.4.1” section.

Introduction

This document provides the following information for FortiSwitch 7.4.1 devices managed by FortiOS 7.4.1 build 2463:

- [Special notices on page 7](#)
- [Upgrade information on page 8](#)
- [Product integration and support on page 9](#)
- [Resolved issues on page 10](#)
- [Known issues on page 11](#)

See the [Fortinet Document Library](#) for FortiSwitchOS documentation.

Refer to the [FortiLink Compatibility table](#) to find which FortiSwitchOS versions support which FortiOS versions.

NOTE: FortiLink is not supported in transparent mode.

The maximum number of supported FortiSwitch units depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitch Units Supported
FortiGate 40F, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E, 91E	16
FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FGR-70F, FGR-70F-3G4G, FG-80F, FG-80FB, FG-80FP, FG-81F, and FG-81FP	24
FortiGate 100D, FortiGate-VM02	24
FortiGate 100E, 100EF, 100F, 101E, 140E, 140E-POE	32
FortiGate 200E, 201E	64
FortiGate 300D to 500D	48
FortiGate 300E to 500E	72
FortiGate 600D to 900D and FortiGate-VM04	64
FortiGate 600E to 900E	96
FortiGate 1000D to 15xxD	128
FortiGate 1100E to 26xxF	196
FortiGate-3xxx and up and FortiGate-VM08 and up	300



New models (NPI releases) might not support FortiLink. Contact [Customer Service & Support](#) to check support for FortiLink.

What's new in FortiOS 7.4.1

The following list contains new managed FortiSwitch features added in FortiOS 7.4.1:

- You can now make your Security Fabric more secure with the FortiLink secured fabric. The FortiLink secured fabric provides authentication and encryption to all fabric links, wherever possible. Zero-touch support is available for FortiLink mode over a layer-2 network and over a layer-3 network.
- More tests have been added to the FortiSwitch recommendations to help optimize your network:
 - When a connected tier-1 multichassis link-aggregation group (MCLAG) peer group is detected and FortiOS detects a possible tier-2 MCLAG pair of switches, FortiOS recommends forming a tier-2 MCLAG.
 - When a connected tier-2 MCLAG peer group is detected and FortiOS detects a possible tier-3 MCLAG pair of switches, FortiOS recommends forming a tier-3 MCLAG.
- You can now enable or disable the locking down of inter-switch links (ISLs) on a single FortiLink interface in the *Edit FortiLink Interface* page (*WiFi & Switch Controller > FortiLink Interface*).
- The FortiOS switch controller now supports the synchronization of the FortiGate system interface description to the switch VLAN description (up to the first 63 characters of FortiSwitch VLAN description field in FortiOS). This allows a more flexible use of the Tunnel-Private-Group-Id RADIUS attribute.
- The CLI commands for configuring Precision Time Protocol (PTP) transparent-clock mode have changed. FortiOS supports the previous CLI commands, as well as the new ones.
- A new CLI command controls whether intra-VLAN traffic is blocked or allowed when the connection to the FortiGate device is lost. Before FortiOS 7.4.1, intra-VLAN traffic on the managed FortiSwitch units was blocked when the connection to the FortiGate device is lost.
- Managed FortiSwitch VLANs can now mirror traffic on a client, and the FortiGate device will analyze the remote traffic.
- Managed FortiSwitch units can now perform inter-VLAN routing. The FortiGate device can program a FortiSwitch unit to do the layer-3 routing of trusted traffic between specific VLANs.
- When using FortiLink mode over a layer-3 network and DHCP discovery with DHCP option 138, the top FortiSwitch unit (with the `_FlinkDhcpDisc_trunk`) will now automatically have a Spanning Tree Protocol (STP) priority of 24576, instead of an STP priority of 32768.

Special notices

Support of FortiLink features

Refer to the [FortiSwitchOS feature matrix](#) for details about the FortiLink features supported by each FortiSwitchOS model.

Upgrade information

FortiSwitchOS 7.4.0 supports upgrading from FortiSwitchOS 3.5.0 and later.

To determine a compatible FortiOS version, check the [FortiLink Compatibility matrix](#).

Within the Security Fabric, the FortiSwitch upgrade is done after the FortiGate upgrade. Refer to the latest [FortiOS Release Notes](#) for the complete Security Fabric upgrade order.

Product integration and support

FortiSwitchOS 7.4.1 support

The following table lists FortiSwitchOS 7.4.1 product integration and support information.

Web browser	<ul style="list-style-type: none">• Mozilla Firefox version 52• Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiOS 7.4.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
848632	After upgrading to FortiOS 6.4.9 or 6.4.10, the link to the managed switch does not come up.
861227	The <i>Device Information</i> column of the <i>FortiSwitch Ports</i> page shows the same device multiple times.
864864	The FortiGate 1500D should not add VLAN TAG 1 for returned decrypted traffic.
893405	FortiLink does not come up for some managed FortiSwitch units after the FortiGate-3600E was upgraded to FortiOS 7.0.10.
897004	On rare occasions, the FortiOS GUI might display blank pages when the user navigates from one menu to another if there is a managed FortiSwitch unit present.
902338	If you configure multitenancy in the CLI and then add another VLAN in the GUI, the VLAN is removed from the other VDOM.
904640	When a FortiSwitch port is reconfigured, the FortiGate device might incorrectly retain old detected device data from the port resulting in unexpected number of detected device MAC addresses for the port. This can result in empty display of the GUI <i>FortiSwitch Ports > Device Information</i> column or <i>Device Inventory and Assets</i> widget.
905795	After upgrading to FortiOS 7.4, random FortiSwitch units are shown as offline in the GUI when they are actually online.
911232	The security rating shows an incorrect warning for unregistered FortiSwitch units on the <i>WiFi & Switch Controller > Managed FortiSwitches</i> page.
920231	When the FortiGate device is rebooted, the configuration for <code>config switch-controller qos ip-dscp-map</code> reverts to the default FortiGate <code>ip-dscp-map</code> values.
936081	When the FortiGate device is rebooted, the VLAN-optimization and <code>vlan-all-mode</code> settings disappear and cannot be restored in the CLI.

Known issues

The following known issues have been identified with FortiOS 7.4.1. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
298348, 298994	Enabling the <code>hw-switch-ether-filter</code> command on the FG-92D model (the default setting) causes FortiSwitch devices to not be discovered.
520954	When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.
527695	<p>Starting in FortiOS 6.4.0, VLAN optimization is enabled by default (<code>set vlan-optimization enable</code> under <code>config switch-controller global</code>). On a network running FortiSwitchOS earlier than 6.0.0, this change results in a synchronization error, but the network still functions normally. If you have FortiSwitchOS 6.0.x, you can upgrade to remove the synchronization error or disable VLAN optimization.</p> <p>On a network with <code>set allowed-vlans-all enable</code> configured (under <code>config switch-controller vlan-policy</code>), the setting reverts to the default, which is disabled, when upgrading to FortiOS 6.4.0. If you want to maintain the <code>allowed-vlans-all</code> behavior, you can restore it after the upgrade.</p>
586801	NetBIOS stops working when proxy ARP is configured and the access VLAN is enabled because FortiGate units do not support NetBIOS proxy.
621785	<code>user.nac-policy[].switch-scope</code> might contain a data reference to <code>switch-controller.managed-switch</code> . When this reference is set by an admin, the admin needs to remove this reference before deleting the <code>managed-switch</code> .
789914	<ul style="list-style-type: none"> When LAN segments are enabled on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models, the internal VLAN (<code>set lan-internal-vlan</code>) is assigned automatically by default. If the same VLAN is configured on the FortiGate device, the configuration fails when it is pushed to the FortiSwitch unit without any warning message. WORKAROUND: Use a custom command. All sub-VLANs must belong to the same MSTP instance if the FortiLink configuration includes the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models.
813216	After CAPWAP offload is enabled or disabled, FortiLink goes down.
814674	When upgrading a FortiAP or FortiSwitch unit that is connected to a downstream FortiGate device, a “Failed to retrieve upgrade progress” message appears.
891642	The FortiGate 6000 and 7000 platforms do not support managing FortiSwitch devices over FortiLink.

Bug ID	Description
910962	<p>After setting values for <code>src-mac</code>, <code>dst-mac</code>, and <code>vlan</code> for the ACL classifier, you cannot use the <code>unset</code> command to remove these settings.</p> <p>WORKAROUND:</p> <ol style="list-style-type: none">1. Remove <code>set acl-group <ACL_group_name></code> from under the <code>config switch-controller managed-switch</code> command.2. Delete the ACL group.3. Delete the ACL.4. Reconfigure the ACL.
940248	<p>When both network device detection (<code>config switch network-monitor settings</code>) and the switch controller routing offload are enabled, the FS-1048E switch generates duplicate packets.</p>



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.